Insert Logo Here

Organization Name

Security Policy

Audit & Accountability

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published AU Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc60976313)

[2 Purpose 1](#_Toc60976314)

[3 Scope 1](#_Toc60976315)

[4 Roles and Responsibilities 1](#_Toc60976316)

[5 Management Commitment 2](#_Toc60976317)

[6 Authority 3](#_Toc60976318)

[7 Compliance 3](#_Toc60976319)

[8 Policy Requirements 4](#_Toc60976320)

[8.1 Audit and Accountability Policies and Procedures 4](#_Toc60976321)

[8.2 Auditable Events 4](#_Toc60976322)

[8.3 Content of Audit Records 5](#_Toc60976323)

[8.4 Audit Storage Capacity 5](#_Toc60976324)

[8.5 Response to Audit Processing Failures 5](#_Toc60976325)

[8.6 Audit Review, Analysis, and Reporting 5](#_Toc60976326)

[8.7 Audit Reduction and Report Generation 6](#_Toc60976327)

[8.8 Time Stamps 6](#_Toc60976328)

[8.9 Protection of Audit Information 6](#_Toc60976329)

[8.10 Audit Record Retention 6](#_Toc60976330)

[8.11 Audit Generation 6](#_Toc60976331)

# Introduction

 has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by management and in compliance with the Audit & Accountability family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

The purpose of these policies is to establish audit and accountability requirements to ensure the confidentiality, integrity, and availability of systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all employees, contractors, third parties, and others who have access to company and customer confidential information within systems and facilities.

# Roles and Responsibilities

These policies apply to all employees, contractors, business partners, third parties, and others who need or have access to systems and our customer's confidential information.

| **Individual or Group** | **Role** | **Responsibility** |
| --- | --- | --- |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Manager | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
|  | System Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

 and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is ’s policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following audit and accountability requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the Organization Name information systems.

## Audit and Accountability Policies and Procedures

This document is intended to serve as the *Audit and Accountability Policy*and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Audit and Accountability Policy*and related physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *Audit and Accountability Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with Organization Name overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Audit and Accountability Policy*and/or procedure(s) must be sent to the Information Owner.

## Auditable Events

 must ensure the information system can audit the following events:

* Successful and unsuccessful account logon events
* Account management events
* Object access
* Policy change
* Privilege functions
* Process tracking
* System events

All web applications must be capable of auditing the following events:

* Administrator activity
* Authentication checks
* Authorization checks
* Data deletions
* Data access
* Data changes
* Permission changes

The security audit function must be coordinated with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events. A rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents must be provided.

Capabilities must be in place to audit additional events based on current threat information and ongoing risk assessment. Reviews and updates of the audited events must occur annually or whenever there is a change in the threat environment.

## Content of Audit Records

Organization Name must ensure that the information system generates audit records that contain, at a minimum, the following information:

* Type of event
* Date and time of the event
* Location of the event
* Source of the event
* Outcome of the event (success or failure)
* Identity of the user/subject associated with the event

Additional audit records must be generated containing the following additional information:

* Session, connection, transaction, and/or activity duration
* The number of bytes received, and bytes sent for client-server transactions
* Additional informational messages to diagnose or identify the event
* Characteristics that describe or identify the object or resource being acted upon

## Audit Storage Capacity

 must allocate audit record storage capacity and configure auditing to reduce the likelihood of capacity being exceeded.

## Response to Audit Processing Failures

Organization Name must ensure that the information system alert designated personnel in the event of an audit processing failure and overwrite the oldest record until the failure is addressed.

## Audit Review, Analysis, and Reporting

Organization Name must review and analyze information system audit records at least weekly for indications of inappropriate or unusual activity as it relates to account usage, privileged access requests, data access requests, and suspicious SQL queries.

Findings must be reported to the designated personnel so adjustments can be made to the level of audit review, analysis, and reporting within information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Automated mechanisms must be employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. Audit records must be analyzed and correlated across different repositories to gain organization-wide situational awareness.

## Audit Reduction and Report Generation

 information system provides an audit reduction and report generation which supports on-demand audit review, analysis, and reporting requirements for after-the-fact investigations of security incidents and does not alter the original content or time ordering of audit records.

Additionally, the information system has the capability to process audit records for events of interest based on successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events as well as resource usage information.

## Time Stamps

 must ensure that the information system executes the following actions:

* Uses internal system clocks to generate time stamps for audit records
* Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets the requirement of one second granularity of time measurement
* Synchronizes internal information system clocks at least hourly with <http://tf.nist.gov/tf-cgi/servers.cgi> when the time difference is greater than 5 seconds
* Selects primary and secondary time servers used by the NIST Internet time service from different geographic regions
* Synchronizes the system clocks of network computers that run Linux-based operating systems to the same time source

## Protection of Audit Information

Organization Name must protect audit information and tools from unauthorized access, modification, and deletion. All audit records are backed up at least once a week onto a different system or media than the system or component being audited. Additionally, authorized access to manage audit functionality is limited to designated personnel only.

## Audit Record Retention

Organization Name retains audit records online for at least ninety (90) days and further preserves audit records offline for a period in accordance with Federal customer and National Archives (NARA) requirements so provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational retention requirements.

## Audit Generation

Organization Name must ensure that the information system executes the following actions:

* Provides an audit record generation capability for the list of auditable events defined in section 8.2 above for all information components where audit capability is deployed.
* Allows the designated personnel to select which events are to be audited by specific components of the system.
* Generates audit records for the list of audited events defined in the policy in Section 8.2 above with the content as defined in the policy for AU-3 in Section 8.3 above